Adapting the Beacon Interval for Opportunistic Network Communications

Salem Sati
Technology of Social Networks Group
University of Düsseldorf, Germany
Email: sati@cs.uni-duesseldorf.de

Kalman Graffi
Technology of Social Networks Group
University of Düsseldorf, Germany
Email: graffi@cs.uni-duesseldorf.de

***Abstract*—A dominant trend nowadays is the rapid spread of small devices, such as laptops and smartphones, carried by people. The users' need for applications with local high-bandwidth requirements and due to limited wireless Internet access, a challenge if identified which is critical for the success of applications such as local wireless data synchronization, gaming or communication. Opportunistic networks provide a solution to localized wireless communication between smart devices. The opportunistic communication between two encountered devices are commonly accomplished by using a radio technology such as Wi-Fi or Bluetooth. One issue involved in device-to-device communication is improving the connection establishment in a mobile opportunistic network with minimum resource consumption. This paper includes a proposal and empirical analysis of the beaconing in opportunistic communication using Wi-Fi technology in the infrastructure mode. With our analysis of the MAC layer, we aim at improving the connection establishment between two adjacent nodes. Precisely, the broadcasting beacon frame is sent by the master device to discover neighbors (stations) at fixed intervals. The contribution of this paper is to propose and evaluate a double hundred kilo beacon interval for opportunistic network communications. The traditional beacon interval is target for low-latency Wi-Fi applications and less suitable for opportunistic networking. The opportunistic networking stations have limited resources and assume delay tolerant applications. Our experiments show that the proposed interval provides a significant reduction in the energy consumption and bandwidth overhead compared to the commonly used beacon interval.**

Keywords: Opportunistic Communication, Neighbor Discovery, Beacon, Infrastructure, Management Frames.

I. Introduction

Nowadays with the rapid growing of the number of smartphones and laptops, the communication based on contact opportunities become more and more viable to implement applications such as wirelessly sharing data in a peer-to-peer manner or local data synchronization. Such networks are of great interest due to the increased number of mobile devices people carry today and the high local wireless bandwidth to each other. On the one hand, these mobile devices have limitations in terms of power, storage and available uplink bandwidth. On the other hand, the application of such networks are characterized as delay tolerant due to lack of predictable connectivity. One application use case is for example the data synchronization between wireless smart devices which benefit from the high bandwidth local connectivity. Another use case is addressing networked virtual environments [1], which allow to converge the real with the virtual world for gaming or augmented reality applications. One potentially successful application might be anonymous file sharing, which might gain large impact [2] on the media industry. In wireless, opportunistic file sharing users specify first their interest of files and their file offerings and then exchange these files over the day during opportunistic contacts. While security issues [3], [4] in these use cases are also relevant, one of the main challenges is defined by the ideal utilization of the random, short opportunistic wireless data exchange times.

This kind of delay tolerant network (DTN) has a high latency due to challenge of intermittent connectivity. One subclass of DTN are opportunistic networks, where communication partners are discovery opportunistically and local, wireless device-to-device communication based on Wi-Fi is used to exchange data. Consecutive routing protocols on the network layer allow to route messages opportunistically to a desired destination. Essentially, Wi-Fi communication can be classified based on the topology and management into two main common types. The first main type is infrastructure, which consists of a central unit that manages the network (Access Point or Wireless Router as master device), in addition to other stations (hand-held devices) such as a smartphone, PDA or laptop, which are connected to the master device. The second type is infrastructure-less, it consists of peers (stations without a master device) which communicate in device-to-device manner in a distributed topology. One option to communicate in an opportunistic network is to enable the nodes to host master nodes in the infrastructure mode while searching for communication partners. Especially in the Android operating system there are limitations regarding the operation of the ad-hoc mode [5].

The idea of the infrastructure mode is built on the master device, this device controls and manages the connection and traffic delivery with connected stations. The IEEE 802.11 [6] has many of standards such as 802.11 b/g standards which both define 11 channels, three of which are non-overlapping (1,6 and 11 channels). The IEEE 802.11 b standards support data rate up to 11 Mbps, where IEEE 802.11 g has a maximum rate of 54 Mbps. Nowadays most carried devices such as smartphones and laptops include a Wireless Network Interface Card (WNIC) which supports both standards IEEE 802.11 b and/or g modes. When these devices enter the coverage area of the master device, then they can establish the connection assuming a strong enough radio signal strength and that they detect the announcement from the master device as a beacon frame. The ISO/OSI model's physical layer represents the radio signal, where the data link layer consists of a MAC sub-layer

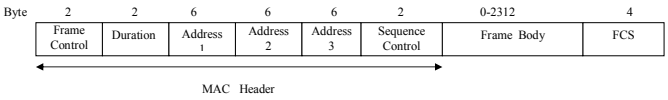


Fig. 1. Management Frame

to manage accessing the medium using CSMA/CA protocol. When the stations need a connection establishment with the master device, they exchange frames, these are generated by the MAC layer of both master device and the station. These frames fall into three main categories: management frames, control frames and data frames. The most important frames, when discovering a neighbor or establishing a connection are management frames. These management frames consist of Probe/Authentication/Association/Re-association request/response frames. Finally, there is the beacon frame which is used by the master device as announcement or broadcasting mechanism for its SSID to all neighbors (stations) in radio range. Moreover, this beacon frame is transmitted by the master device at fixed intervals. This paper analyzes the impact of the beaconing on opportunistic networking and proposes enhancement of the Wi-Fi communication based on infrastructure as a technology of mobile opportunistic communication and neighbor discovery. In Section II we discuss the functionality of opportunistic communications and neighbor discovery. Here the details of the IEEE 802.11 standard are of high relevance, which we discuss in Section III. We propose in Section IV an analysis of the functionality of the beacon frame and introduce our approach. Section V presents related work in adapting the beacon interval. Furthermore, Section VI includes the metrics and tools used to gather the data from the experiment scenarios. In Section VII we investigate the results of the experiment scenarios of comparing the proposed beacon interval with traditional beacon. Finally, Section VIII gives the conclusion and future work.

II. Opportunistic Network Communications

Mobile opportunistic communications are formed between mobile devices using radio frequency technologies such as IEEE 802.11 or Bluetooth. To detect if there is any devices (Neighbor) around a node to communicate with, a device needs to send beacons (active mode), or listen for beacons (passive mode) sent by others. This task is costly in terms of energy, bandwidth, and delay. The opportunistic middleware is often implemented as application layer, using the interfaces of the platform / operating system. Therefore, it is important to know the behavior of the device-to-device communication in such an environment of mobile opportunistic communication in user-space. It is also very important to look at the operation system (platform assumption) where it is the that kernel space will handle the device discovery based on the wireless technology available, such as infrastructure-based Wi-Fi. This importance comes from that the connectivity manager is the responsible component in the mobile opportunistic stack. The connectivity manager makes the interfacing between the user and kernel spaces. The DTN middleware runs on the top of the platform (operating system), therefore, improvements to the opportunistic communication and neighbor discovery are required below this point.

III. Background on Beaconing in IEEE 802.11

The IEEE 802.11 Working Group was founded in 1990 to specify standards for Physical (PHY) and Medium-Access Control (MAC) layers for WLANs. The IEEE 802.11 evaluated through a number of generations [6]. The old common standards of wireless networks were 802.11 b and g. The goal of the Task Group b was to increase the maximum bit rate in the 2.4 GHz frequency range. The IEEE 802.11g is working on an extension to IEEE 802.11b at 2.4 GHz for enabling the data transmission at rates up to 54 Mbps. One main objective in (wireless) opportunistic networking is to support emerging contacts and thus to quicken the connection time. One option to setup a connection is to operate a node in infrastructure mode and to announce the presence through beacons.

In general, the wireless infrastructure mode of the IEEE 802.11 is organized by the master device through neighbor discovery and connection phases. The master and station devices are sending and receiving MAC management frames as Figure 1 shows. The beacon frame is one of the management frames and is used as broadcasting frame to announce the SSID of the master device. Moreover the master device transmits the beacon frame at a fixed rate, therefore, most of Wi-Fi vendors configure by default their products with this traditional fixed beacon interval. This interval is determined based on a so-called Time Unit (TU), with most vendors setting $TU = 1024\mu s$. The default value for most vendors nowadays is 100 TU, the default traditional beacon interval is therefore calculated as 102.4 milliseconds. This beacons frame is sent by the master device which supports IEEE 802.11 b and/or g at rate of 1 Mbps, whatever the actual data rate is. This behavior of the master device of periodically broadcasting the beacon frame is considered as active scan discovery for neighbors.

Based on that the beacon frame is sent at a rate of 1 Mbps in IEEE 802.11 b or g, the bit time is calculated as one microsecond. The delay resulting from different layer encapsulations is measured in different time units as shown in Figure 2. In addition, the Protocol Data Unit (PDU) at different TCP/IP layers will add to the delay. This delay will increase based on the construction of the TCP/IP stack, where the PDU will be sent to upper layers via SAP port in a sequential fashion. The cumulative delay of PDUs is measured at different layers in different time units, for example the frames and packets operate at the time unit of a microsecond, while the delay at the TCP/UDP segments and middleware programs (as opportunistic networking or delay tolerant networking (DTN) bundle) will be at the unit of a millisecond. On the top of the TCP/IP stack, at the application layer, the low-latency and MANET application will operate at the time unit of a second. Finally, on the top of the Figure 2 the high-latency DTN applications will operate with the time unit of a minute. Based on the DTN applications which are delay tolerant, we make a trade-off between the power consumption as limitation of a DTN station and the delay which is one characteristic of opportunistic networks.

The contribution of this paper is to propose and evaluate an adapted beacon interval for the opportunistic communication and energy-efficiency neighbor discovery using Wi-Fi technology in the infrastructure mode. In specific, we increase the beacon interval to minimize the power consumption of the WNIC and to improve the channel utilization. We investigate the impact of increasing the beacon interval on the opportunistic device-to-device communication in Section VII. The default value of a fixed beacon interval is equal to 100 TU or 102.4

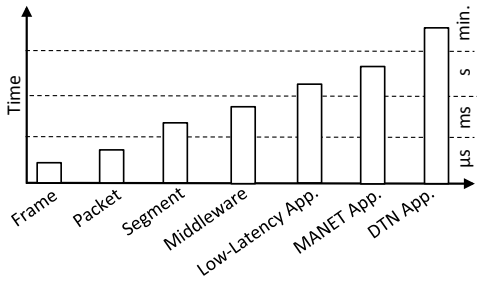


Fig. 2. Delay of different Data Units

milliseconds, defined for WLANs as a trade-off between the device's requirements on mobility, power saving and contact probability, and the application requirement of low-latency and real-time support which impact the end-to-end delay.

In most of commercial master Wi-Fi devices supporting 802.11 b and/ or g, the beacon interval by default has a fixed value of 102.4 millisecond or 100 TU, moreover, most vendors make this interval configurable as advanced wireless setting. This feature enables the user to modify the fixed beacon interval as integer multiple of kilo-microsecond. This integer may range from 20 to 1000 and is defined in the vendor's or appliance firmware's parameters. The user can configure the this interval to a value other than the default fixed value of 100 TU. Before we analyze the impact of modifying the default beaconing interval, we discuss the question of why the default interval is chosen as 100 TU or 102.4 milliseconds.

IV. Proposal of a 2HKBI Beacon Interval

The beacon interval should consider following factors. The first influencing factor is mobility and roaming delays which impact on end-to-end delays of real-time applications such as Voice-over-IP (VoIP). The VoIP application requires that the maximum allowable delay should be in range of 102.4 millisecond [7], such that a beacon interval greater than 102.4 will result in a higher delay. This delay comes from de-association and re-association of the station with a new master device, moreover, the delay may lead to de-authenticate when it becomes higher than the connection timeout. On the other hand it may be better to let the interval be less than 102.4 millisecond, but then the energy efficiency problem due to the power consumption and a high of overhead occurs which mean a poor bandwidth utilization. The second factor is related to the bandwidth. When the beacon interval is set to the default value of 102.4 milliseconds, the number of beacon frames will be around ten frames per second. By increasing the time of beacon interval the channel utilization will be increased and vice verse, as discussed in [8]. Moreover, the management frames are considered as overhead and induce a delay from the application view. This delay and overhead leads to low packet delivery ratio as shown in [9]. Regarding the power safe mode (PSM), point three in the list, the default value is selected based on the PSM mode as trade-off between power consumption and delay of low-latency application, see [10]. When the transmutation rate of management beacon frames is increased, it results in a higher power consumption. When the beacon rate is decreases to a value less than the traditional rate, it leads to a high delay with low bandwidth as discussed in [11]. Therefore, a power save mode is chosen as trade-off between power consumption and the bandwidth [12]. The fourth impact of the beacon interval is the delay of the single-hop discovery of neighbors. The default value of 1.024 milliseconds, selected as an application-defined requirement of having the contact miss probability of less than 10% [13], corresponding to the fifth point in the list. This probability is suitable for communication environments of low latency applications. Finally, the beaconing interval is based on the Time Unit and Kilo-microsecond relationship. From the perspective of the Ethernet technology, the TU interval of Kilo-microsecond is twice the minimum Ethernet frame length of 64 bytes. Moreover, in high delay applications, the infrastructure-based wireless network uses a preamble frame length of 148 microseconds. The long preamble frame is around twice the length of the short preamble frame of 72 microseconds. This short preamble frame is targeted at low latency Wi-Fi applications.

We propose to set the beacon interval of the master device in the infrastructure-based mobile opportunistic networks to be twice the traditional interval of a commercial Wi-Fi appliance, namely 204.8 milliseconds or 200 TU, which we term Double Hundred Beacon Interval (2HKBI). With this modification, we aim at improving the opportunistic device-to-device communication and to induce an energy-efficient neighbor discovery.

V. Related Work

The beacon interval is very important for any kind of wireless communication. The main function of the beacon is signaling the availability in the network, keeping the device alive and to detect new devices. Most wireless communication devices suffer from limitations of battery and bandwidth. Therefore, the beacon interval should be chosen with specific time calculation balancing between a long interval saving energy, on the one hand, which means a delay in neighbors discovery and application latency, and a short interval on the other hand, which leads to high power consumption and poor channel utilization (overhead). The beacon interval is also critical for the wireless infrastructure and infrastructure-less modes of the IEEE 802.11 standards. There is no specific value defined for the beacon interval. For wireless HTTP clients, [14] investigates the impact of the beacon interval on the throughput. The author makes the interval dynamic based on the RTT value of the packet. In opportunistic networks, there are some proposals to set the beacon within a few seconds. While the interval of a beaconing frame is not specified in the DTN-IPND protocol [15] description. This beaconing interval is proposed as adapted to different mobility-awareness configurations [16], where the beacon interval equals 2 seconds when the speed of the node equals 0 m/s (static). The beacon interval is equal to 0 when the speed of the node greater than 0 m/s (dynamic). Moreover, in [17] the author propose scenarios of access-point-based opportunistic network topologies such as WiFi-Opp Static, Flexible STA, Flexible AP and Fixed APs with real-world mobility traces of smartphones. The authors assume the scanning time equal to passive and active scanning time and calculate the epidemic dissemination performance regarding the beacon interval in time unit of one second. The graphs, however, show that the beacon interval should be kept shorter less than 2 second to get 50 % less power consumption. In [18] the authors present a hardware and software architecture for energy-efficient throw boxes in DTNs. They show that a single throw-box with solar panel can run with improving

of packet delivery by 37 % and reducing message delivery latency by at least 10 % in their prototype. Moreover, to achieve these values they assume that the mobile nodes beacon their position, speed, and direction at fixed time intervals in their prototype, namely once per second. A fixed beaconing approach optimized in terms of throughput for an energy-constrained network has been studied in [18], where the beacon transmission is controlled by introducing three node states which are inactive (not participating in communication), active (beaconing) and infected (not beaconing). A power saving modes using both low- and high-power radio is proposed in [19] where the short-range radio is used to discover contacts (alternating between sleep and awake modes), while the data transmissions is done by high-power radio.

In this paper we investigate the impact of the timing of the beaconing with respect to the IEEE 802.11 standard for the application use case of an opportunistic network. Next, we discuss the metrics and tools to measure the impact of the beacon interval on the contact establishing time, the bandwidth and the power usage.

VI. Tools and Metrics

In order to evaluate the performance of the proposed beacon interval 2HKBI in comparison with the traditional beacon interval of 100 TU, in this section we present our evaluation methodology. We considered the mobile opportunistic scenario in which a neighboring node is detected and a connection is established with one station node and a single master device. We use a monitor node to capture MAC frames for analysis. To evaluate the performance of the two considered beacon intervals, we measured a set of metrics by the following tools.

A. Tools

The Linux wireless kernel has a driver for most commercial WNIC. It uses the Wireless Extensions to simplify the configuration and the statistical data capture at the kernel space. This wireless extension gives the user the ability to monitor the internal physical and MAC events to the system log using Netlink sockets between user and kernel spaces. We utilized a set of relevant tools that can be used to perform the measurement tasks such as capturing, processing time and monitoring. The Linux Wireless Extensions form a generic API allowing a Linux kernel to communicate with the user space. This set of tools creates a socket interface at the user space to configure, control, query and debug the WNIC. A common usage example of these tools is access the WNIC statistics using *iwconfig*, while *iwspy* allows users to check the per node link quality. The *iw* event can be used as monitoring tool which sends reports of WNIC events to the console. Moreover, there is *dmesg* tool to monitor all Linux kernel messages and events which can be used to measure times between different events. *WaveMon* is a wireless monitoring tool that can be used for measuring the received signal strength in addition to link quality of connection. It allows the real time monitoring of the signal, noise levels, packet statistics and WNIC configuration. During an experiment, *WaveMon* offers two different views: A current state snapshot of the WNIC, link statistics and a historical graph for the same parameters. *Wireshark* (formerly *Ethereal*) is an open source tool of to analyze network traffic. It integrates a packet sniffer and analyzer tool for wired or wireless networks. Further, it includes very powerful packet and frame capturing and filtering tools. Specific filters can be built based on the field of the captured packet or frame. However, Wireshark offers capturing list uses coloring filters, which help to identify faster which type of packets or frames are present. It also includes a capture timestamps feature which comes from the *Winpcap* packet capture library. We used these tools to capture the following metrics.

B. Metrics

The beaconing function has impact on the connection time, on the power consumption and the resulting available bandwidth, therefore, we will measure these metrics.

1) Connection Time and One-Hop Delay: The beacon interval being a time value has influence on further time values, which we measure:

1) Time consumed to establish the connection (neighbor discovery and connection phase).
2) One hop end to end delay.
3) Probability of missed contacts.

For the calculation of the time to establish a connection between two nodes, we consider two steps: neighbor discovery and connection. We define the *time of discovery* as the sum of the time consumed from the initial station starting to scan, to find the SSID, to finish the scan, until the kernel message arrives of a new station detected. The *time for the connection* starts from the authentication, followed by association with the master and finally the connection phase. The time is finished when the kernel notifies that the connection to the master device is ready. These times indicate how much time is consumed discovering the neighbor node with both intervals, the performance is be measured for separate phases. In addition to the connection establishment, the *one hop end-to-end delay* is relevant. We calculate this time as the average time between the creation of a frame with a specific sequence number in memory at the sending and receiving site. Finally, we calculate the probability of missed contacts, we capture the beacon frames in different time slots for both traditional and 2HKBI intervals. We assume that DTN applications require the discovery probability being at least 90%, i.e. the probability of missed contact must be less than 10%. The beacon frame's main function is an SSID announcement by a master device which should be heard from neighboring stations. Therefore, we assume that a missed contact is as missed beacon frame. The probability of a missed contact is calculated as follow:-

$$P = (\frac{No\ \ Beacons - Captured\ \ Beacons}{No\ \ Beacons})$$

2) Bandwidth and Utilization: This metric includes the process for computing the traffic generated through management frames used in the neighbor discovery and connection phases. In specific we count in all overhead messages such as beacons, probe requests, probe responses, association requests and responses, authentication requests and responses. We assume that the station behavior model is on an average of the normal wireless station which sends two probe requests per minute per channel. One of these is a broadcast with SSID set to the broadcast ESSID and the other frame is sent with the ESSID set to the required SSID which is selected by the user or may by the RSSI signal strength. The required SSID probe request is a broadcast but only the specific master

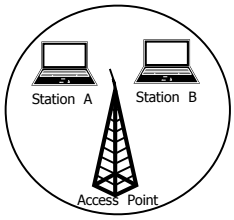


Fig. 3. Experiment Scenario

TABLE I. SCENARIO CONFIGURATION

Parameter	Value
Beacon Interval	100, 200 TU
Tx Power	20 dBm
PSM mode	disabled
Channel	auto
Bit rate	auto
Security	disabled
IEEE 802.11 mode	b /g
RSSI	-70 dBm
Link Quality	39/70

TABLE II. CAPTURED MANAGEMENT FRAMES

Name of Frame	Frame Size in Byte
Beacon	77
Probe Request	223
Probe Response	71
Auth. Request	48
Auth. Response	48
Assoc. Request	60
Assoc. Response	54

TABLE III. COMPARISON BETWEEN TRADITIONAL 100 TU AND OUR 2HKBI

Neighbor Discovery and Connection Phases Times

Parameter	Beacon 100 TU	2HKBI
Discovery phase (sec)	1.050	1.053
Connection phase (sec)	0.010148	0.010168

Bandwidth Utilization and Overhead

Parameter	Beacon 100 TU	2HKBI
Bandwidth Mbps	0.006	0.003
Utilization	0.006	0.003
Frames	557	274
Bytes	42889	21098

device with the corresponding SSID would respond. The master device is pre-configured with the SSID and one of both beacon intervals, namely the traditional beacon interval or our proposed 2HKBI. At the same time, the behavior of the master device is configured to respond to broadcast probe requests for any nearby station. In the bandwidth calculations, we assume the following. The beacons and other management frames are transmitted at the lowest supported rates which would be 1 Mbps for a 802.11 b/g network. The frames lengths are as listed in Table II for the calculations of the bandwidth consumption and channel utilization. All beacon frames are considered, in addition, the interference probe responses of specific master device are also considered.

3) Power Consumption: The power consumption is critical in DTN stations. Therefore, we calculate the power consumption of receiving the management frames at the station. The scanning process of the station for a master device consumes a significant percentage of the total device power consumption. Three types of scanning are identified. First, *active scanning*, in this kind of scanning the station sends a probe request and receive a probe response from the master device on that channel. Second, the *passive scanning*, in this scanning the station waits on a channel to receive the beacon frame from the master device. Third, immediate scans for network discovery. *Discovery scan* is a series of scans on all channels to discover all available master devices. Passive scanning leads the station to wait on the channel for receiving the beacon frame which is sent periodically by the master device. By this, more station energy is wasted. The delay of passive scanning is calculated as:

$$Max\ Delay = No\ \ Channels \times Max\ \ Beacon\ \ Interval$$

On the other hand, active scanning requires the transmission of probe requests and adds more power consumption as immediate scan impact. So, we measure the power consumption based on scan time as battery usage, moreover, we assume that the Power Saving Mode is disabled, as Table I shows. Next, we describe our experiment setup and the evaluation results.

VII. EXPERIMENT SCENARIO

The efficiency and performance of the proposed 2HKBI for opportunistic device-to-device communications has been evaluated through a series of experiments, where two portable devices (laptops) and one master devices are used to build the experiment scenario. The experiment setup is sketched in Figure 3. These devices were operated with Linux operating systems. Device A works as DTN station where device B works as monitor station. Station A communicates using WNIC (with rt2800pci chip-set) to establish the connection with the master device (Access Point). The parameter settings used in our experiments are shown in Table I. They are considered sufficient for an adequate configuration of the proposed 2HKBI in order to experimentally analyze the delay, bandwidth and energy benefits. The experiment compares the impact of two beacon intervals, traditional 100 TU and 2HKBI, on the infrastructure-based opportunistic communication and neighbor discovery. The parameters of the channel selection was kept as auto to give the access point ability to change the frequency for interference and delay of scanning. Also, the bit rate was auto as default, because the management frames rate is fixed at low rate of 1 Mbps. The master device is selected in the experiment as an access point, this access point has a configurable beacon interval, we changed this value between the traditional value of 100 TU and the proposed 2HKBI value of 200 TU. The Power Save Mode is disabled, as our research focuses on the performance of neighbor discovery and opportunistic device-to-device communication.

Station A has WNIC which operates in IEEE 802.11 b/g/n mode at 2.4 GHz. The monitoring device B works as a frame sniffer to capture the 802.11 management traffic by forcing the WNIC to operate in monitor mode instead of management mode. The sniffer tool used is Wireshark, it has been very valuable to monitor and analyze the device-to-device communication performance. In specific, we aim to measure the management traffic generated by master device and station A, this traffic consists of frames as shown in Table II. The beacon frame has length of 77 Byte which is close to minimum Ethernet frame of 64 Byte, but it still consuming the bandwidth and energy of the opportunistic devices. The length of a Probe requests of station A seems to be large (223 Byte) as it has WNIC support IEEE 802.11 b/g/n mode.

We conducted a set of over-the-air measurements with ten iteration for each experiment for more accuracy. We measure link quality through the Received Signal Strength Indication (RSSI) value based on the impact of this parameter on the opportunistic communications distance and performance. The RSSI is around -70 dBm (Link quality is 39/70). We assume that it allows relatively large communication distances between opportunistic devices with good performance levels.

A. Connection Time and One-Hop Delay

The beacon frame's function is to broadcast the SSID of the master device periodically for minimizing the miss contact probability and connection establishment delay. A highly frequent broadcast, i.e. small beacon interval, would minimize this delay. On the other hand, we have DTN stations which are suffering from resource limitations, such as battery and bandwidth, thus an increased beacon interval is suggested. To resolve this tradeoff, we compare the impact of increasing the beacon interval on opportunistic communication.

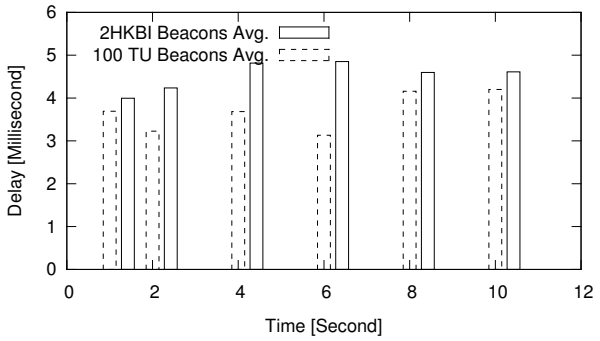


Fig. 4. One-hop Delay

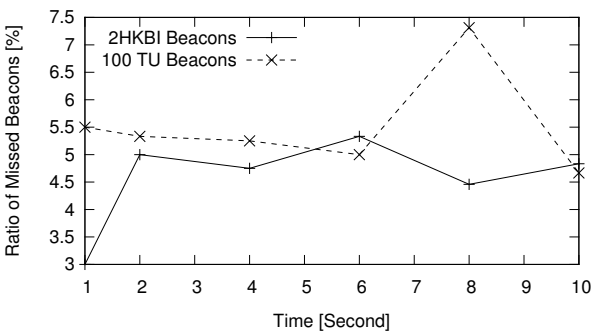


Fig. 5. Miss Contact Probability

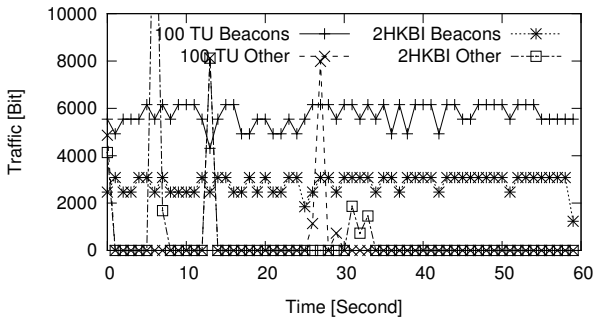


Fig. 6. Management Traffic generated by both Beacon Intervals

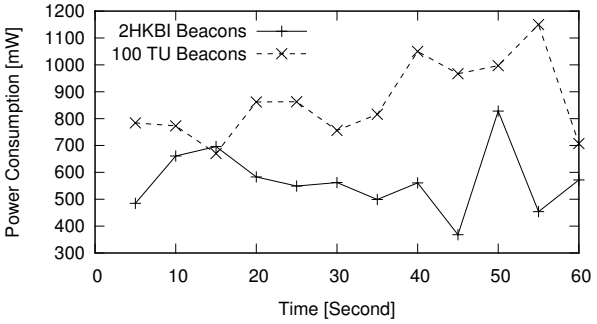


Fig. 7. Power Consumption

Device-to-device opportunistic communications consist of two phases: the neighbor discovery depending on the time of hearing the beacon frame and the connection phase which is done through the exchange of authentication and association frames. We assume in the experiment that the neighbor discovery phase starts when station A starts active scanning of the channels, this phase ends when the kernel notifies that a new station is detected. The connection phase is finished when the kernel-space notifies that the station A is connected to the master device. We measure the active scanning time of the station A using the *iw* tool, it takes around 1 second to scan 11 channels. Moreover, we use the *dmesg* tool to monitor the wireless events at the kernel-space.

We depict the average time for both phases in the Table III. The delay of using 2HKBI compared to traditional 100 TU is around 3 ms which results from the processing time in kernel space, as the passive scanning time of station A is still equal to 100 millisecond for both beacon intervals at the master device. The connection phase has the same performance, as this phase is not depending on the beacon frame interval.

The other impact of the beacon frame interval is on the one-hop delay. We measure this time as the delay to duplicate frames sent by the master device with a same sequence number in memory of the receiver. The opportunistic middleware uses message routing based in a context-centric store-carry-forward fashion over a host-centric packet switching routing. Underlay layers should consider one-hop instead of multi-hop routing. We depict the one-hop delay time for both the traditional and our proposed 2HKBI beacon interval in Figure 4. The graphs shows that the maximum difference in delay between the two beacon intervals is around 2 ms which it complies to high latency application requirements named in [20].

A further impact of the beacon interval is on the miss contact probability for which we assume as miss of a beacon frame. We captured the (missed) beacon frames for different slots of times, and calculated the probability of missed contacts. In Figure 5 we depict the probability of missed contact. The results for the proposed 2HKBI approach are very similar to the results of the traditional beacon interval with less than 10 %. This is because both beacon intervals times are still small (102.4ms and 204.8ms) when compared with the total channel scan time in the neighbor discovery phase (roughly 1s). The succeed contact probability of 90% corresponds Whit DTN application requirements.

B. Bandwidth and Utilization

Reducing unnecessary or inefficient management traffic reduces the channel utilization, therefore, removing the extra or unnecessary management traffic improves the available bandwidth and reduces the power consumption. In fact, the beacon frame traffic generated is greater than other management frames required for neighbor discovery and opportunistic device-to-device communications. The bandwidth benefits can be achieved by exploiting the management frames traffic generated by the opportunistic device-to-device communications and analyzed by means of the total number of radio frames transmitted between station A and the master device (AP) for neighbor discovery and connection establishment phases. We aim to identity the total number of radio frames classified as beacon frames in comparison to other frames which are authentication and association frames.

For our scenario, we configure the master device with traditional beacon interval of 100 TU. Then we capture through the monitoring node B the management frames exchanged between the master device and the station A. Figure 6 shows the traffic overhead for the traditional and the 2HKBI beacon interval during a time of 60 seconds. The traffic generated by the beacon frame is in average 5708 bps for the 100 TU interval and 2804 bps for the 2HKBI interval. Using the 100

TU interval, at time $t = 13s$, station A detects the master device and requires to join the SSID of this master device. The management frames generated a traffic of 8120 bps in this point of time. This traffic results from the authentication and association frames exchanged between the master device and the station A. Using the 2HKBI interval, at time $t = 6s$, we observe the event when the station A negotiates the connection with the master device. This event generated a traffic burst of 18254 bps for connection establishment, resulting from the authentication and associate steps, in addition of duplicate probe response from the master device.

We calculate the traffic rate for both beacon intervals, as the Table III shows. The utilization of the proposed 2HKBI approach is 51 % improved in respect to traditional beacon interval, with 0.003 Mbps in comparison to 0.006 Mbps. Assuming a channel rate at 1 Mbps for transmitting the management frames in IEEE 802.11 b/g, the channel utilization is 0.003% and 0.006%, respectively.

C. Power Consumption

In order to perform an energy consumption analysis, we measure the real energy of the management frames transmigration for both traditional and 2HKBI intervals. We measure how much energy they consume when Wi-Fi is in an ideal state. The energy measurements is shown in Figure 7 is sampled every 5 seconds in a one minute time slot. The energy consumption of transmitting management frames is represented as a mW unit. The energy consumption is mainly impacted by the scanning time and the beaconing interval. Therefore, we measure the power consumption of passive scanning of station A which is impacted by the active scan of beacon frames sent by the master device. Figure 7 demonstrated that most energy is required for received beacons frames with the traditional beacon interval. With our proposed 2HKBI less useless SSID beacons frames as sent and energy is conserved.

To analyze the impact of the beaconing interval on the energy consumption, we sampled the WNIC energy consumption as reference to the same station A battery. As the Figure 7 illustrated, the power consumption average for a traditional beacon interval is around 866 mW, where for the proposed 2HKBI it is around 568 mW. This means improving the power efficiency of around 35 %, this improvement mostly results from reducing the beacon frame transmigration rate by the proposed 2KHBI beacon interval.

VIII. Conclusion and Future Work

In this paper, we address the problem of mobile opportunistic communications and neighbor discovery using Wi-Fi technology. We have shown that the energy and bandwidth efficiency of opportunistic communications can be significantly improved using an proposed approach based on duplicating the traditional beacon interval. We propose a beacon interval of 200 time units or 204.8 ms, termed Double Hundred Beacon Interval (2HKBI), in which beacons are emitted by the master device to announce its SSID. We have analyzed the performance of the proposed 2HKBI approach, in an empirical scenario in a simple test-bed. The obtained results show that the proposed approach can provide a significant energy conserving and overhead reduction with respect to the traditional beacon approach of 100 TU or 102.4ms. The proposed approach can reduce the overhead by up to 51 % with the same miss contact probability as the traditional beacon interval. Moreover, the proposed 2HKBI approach improves the energy-efficiency of around 35 % in infrastructure-based opportunistic device-to-device communications. In future, we aim to investigate the impact of the 2HKBI approach on the efficiency of the Power Save Mode and on duty cycling of mobile opportunistic communications.

References

[1] A. Kovacevic, K. Graffi, S. Kaune, C. Leng, and R. Steinmetz, "Towards Benchmarking of Structured Peer-to-Peer Overlays for Network Virtual Environments," in *IEEE ICPADS'08*, 2008.

[2] N. Liebau, K. Pussep, K. Graffi, S. Kaune, E. Jahn, A. Beyer, and R. Steinmetz, "The Impact Of The P2P Paradigm on the New Media Industries," in *AMCIS*, 2007.

[3] P. Mogre, K. Graffi, M. Hollick, and R. Steinmetz, "AntSec, WatchAnt and AntRep:Innovative Security Mechanisms for Wireless Mesh Networks," in *IEEE LCN '07*, 2007.

[4] P. S. Mogre, K. Graffi, M. Hollick, and R. Steinmetz, "A Security Framework for Wireless Mesh Networks," *Wireless Communications and Mobile Computing*, vol. 11, no. 3, pp. 371–391, 2011.

[5] T. Zhuang, P. Baskett, and Y. Shang, "Managing Ad Hoc Networks of Smartphones," *International Journal of Information and Education Technology*, vol. 3, no. 5, 2013.

[6] IEEE Standard 802.11, Part 11, "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications," http://standards.ieee.org/about/get/802/802.11.html, 2007.

[7] O. H. Sabrie, "Fast Handoff for 802.11 Wireless Network," *Communications and Network*, vol. 03, no. 04, pp. 250–256, 2011.

[8] J. Kwak, H. Lee, and K. Lee, "A Study on the Airtime occupied by Beacon Frame in 802.11 Hotspot Environment," in *Proc. of the KICS'12*, 2012, pp. 11–12.

[9] M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, and J. Zahorjan, "Measurement-based Characterization of 802.11 in a Hotspot Setting," in *Proc. of the ACM Workshop on E-WIND'05*, 2005, pp. 5–10.

[10] J. Lee, C. Rosenberg, and E. K. P. Chong, "Energy Efficient Schedulers in Wireless Networks: Design and Optimization," *ACM Springer Mobile Networks and Applications (MONET)*, vol. 11, no. 3, pp. 377–389, 2006.

[11] Y. Xie, X. Luo, and R. K. C. Chang, "Centralized PSM: An AP-centric Power Saving Mode for 802.11 Infrastructure Networks," in *Proc. of the Int. Conf. on Sarnoff Symposium (SARNOFF'09)*, 2009, pp. 375–379.

[12] A. Gupta and P. Mohapatra, "Power Consumption and Conservation in WiFi Based Phones: A Measurement-Based Study," pp. 1–10.

[13] M. Emmelmann, S. Wiethoelter, and H.-T. Lim, "Opportunistic Scanning: Interruption-free Network Topology Discovery for Wireless Mesh Networks," *Proc. of WoWMoM'09*, pp. 1–6, Jun. 2009.

[14] S. Nath, Z. R. Anderson, and S. Seshan, "Choosing Beacon Periods to Improve Response Times for Wireless HTTP Clients," in *Proc. of MobiWac'04*, 2004, pp. 43–50.

[15] R. Altmann and A. Gladd, "DTN IP Neighbor Discovery (IPND)," https://tools.ietf.org/html/draft-irtf-dtnrg-ipnd-02, pp. 1–26, 2014.

[16] A. Hess, E. Hyytiä, and J. Ott, "Efficient Neighbor Discovery in Mobile Opportunistic Networking using Mobility Awareness," in *Proc. of COMSNETS'14*, 2014.

[17] S. Trifunovic, B. Distl, D. Schatzmann, and F. Legendre, "WiFi-Opp: Ad-hoc-less Opportunistic Networking," in *Proc. of ACM CHANTS '11*, 2011, pp. 37–42.

[18] N. Banerjee, M. D. Corner, and B. N. Levine, "Design and Field Experimentation of an Energy-Efficient Architecture for DTN Throwboxes," *IEEE/ACM Trans. on Networking*, vol. 18, no. 2, pp. 554–567, 2010.

[19] H. Jun, M. H. Ammar, M. D. Corner, and E. W. Zegura, "Hierarchical Power Management in Disruption Tolerant Networks with with Traffic-Aware Optimization," *Computer Communications*, vol. 32, no. 16, pp. 1710–1723, 2009.

[20] J. Su, J. Scott, P. Hui, J. Crowcroft, E. de Lara, C. Diot, A. Goel, M. Lim, and E. Upton, "Haggle: Seamless Networking for Mobile Applications," in *Proc. of UbiComp'07*, 2007, pp. 391–408.